PART5　暗号化とデジタル署名

目標
- 暗号化方式やデジタル署名について理解する。
- それぞれの暗号化方式の特徴について説明できる。

Chapter1　暗号化とデジタル署名

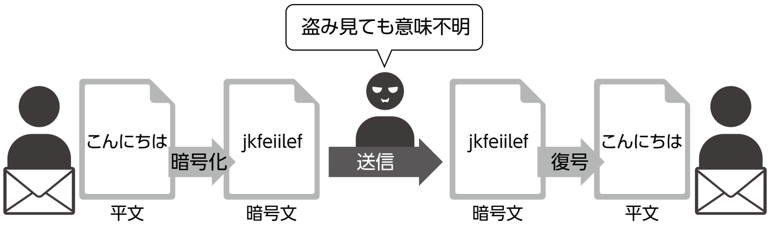
暗号化（共通鍵暗号方式と公開鍵暗号方式）

• 暗号化と復号

情報通信ネットワーク上では，さまざまなデータがやり取りされている。そのデータが本来送りたい相手ではない第三者に盗聴されたりして，中身が知られてしまう被害を防ぐためには，データを第三者に解読できないものにする必要がある。

データの内容を第三者に解読できないものにする技術または手法のことを〔①　　　　　　〕という。暗号化されたデータを元のデータに復元することを〔②　　　　　〕という。

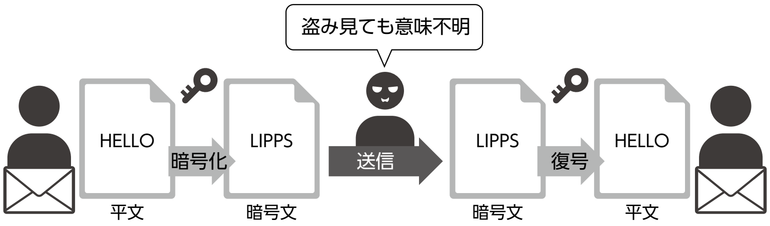
覚えておこう
暗号化する前のデータを平文（ひらぶん），暗号化後のデータを暗号文という。



• 共通鍵暗号方式

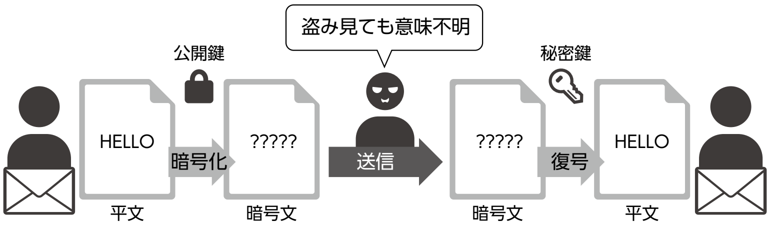
暗号化に使う鍵と復号に使う鍵が同じ方式のことを〔③　　　　　　　　〕という。送信者と受信者が何らかの方法でお互い同じ鍵（〔④　　　　　　〕）をあらかじめ共有しておく必要がある。

覚えておこう
ここでいう「鍵」とは暗号化や復号の時に使うデータのことである。



• **公開鍵暗号方式**

〔⑤　　　　　〕と〔⑥　　　　　〕の 2 種類の鍵（鍵ペア）を用いて暗号化・復号を行う方式のことを〔⑦　　　　　〕という。公開鍵で暗号化したデータは，対応する秘密鍵でのみ復号できる。



• **共通鍵暗号方式と公開鍵暗号方式のメリット・デメリット**

	共通鍵暗号方式	公開鍵暗号方式
メリット	公開鍵暗号方式に比べて，暗号化と復号が〔⑧　　　〕	公開鍵は公開情報なので，漏洩しても問題ない（受け渡しが容易）
デメリット	複数の人とデータをやり取りする場合，人数分の異なる共通鍵を準備し，これを安全に共有し使い分ける必要があり，鍵の管理が大変になる	共通鍵暗号方式に比べ，暗号化と復号に〔⑨　　　〕

デジタル署名

• **ハッシュ値（メッセージダイジェスト）**

元のデータをハッシュ関数に入れて求めた一定の長さの値のことを〔⑩　　　　　〕という。ハッシュ値から元の値に戻すことは不可能で，元のデータを推測することもできない。ハッシュ値は文書の改ざん検知に用いられる。

知っておこう

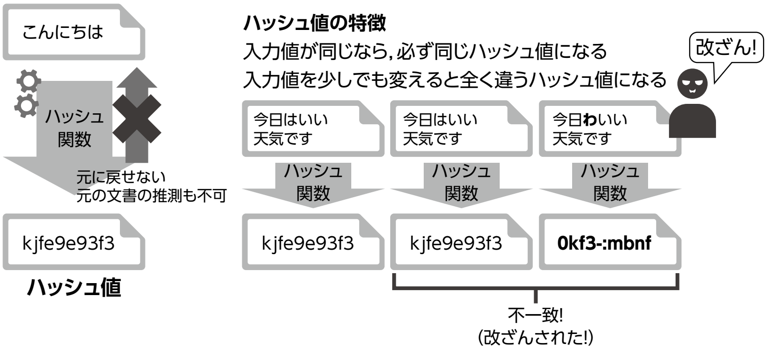
秘密鍵は秘密の情報なので外部に漏らしてはいけない。一方，公開鍵は公開してよい情報になる。そのため，公開鍵は，受け渡しが容易に行える。

ここが POINT

公開鍵暗号方式では，公開鍵が閉める専用の鍵（暗号化）で，秘密鍵が開ける専用の鍵（復号）である。

覚えておこう

送信者は，公開鍵を生成するとき，認証局（CA）という第三者機関に公開鍵を登録することによって，公開鍵が本人のものであることを証明してもらえる。これをデジタル証明書や公開鍵証明書という。受信者は，そのデジタル証明書を用いて公開鍵が本物（送信者本人の物）であることを確認できる。



- **デジタル署名**

〔⑪　　　　　　　　　〕：公開鍵暗号方式とハッシュ値を利用して，送信されてきたデータが間違いなく本人（送信者）のものであること，改ざんされていないことを証明するための技術。

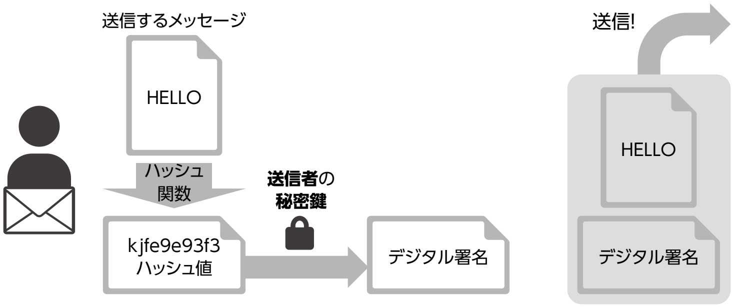
【送信者側の処理】

(1) 送信するメッセージをハッシュ関数に入れて，ハッシュ値を求める。

(2) そのハッシュ値を，自らの秘密鍵を用いて署名する。これをデジタル署名と呼ぶ。

(3) 送信者は，送信するメッセージとデジタル署名を受信者へ送付する。

知ってておこう
ここで紹介したのは，デジタル署名の代表的な 1 つの方式である。



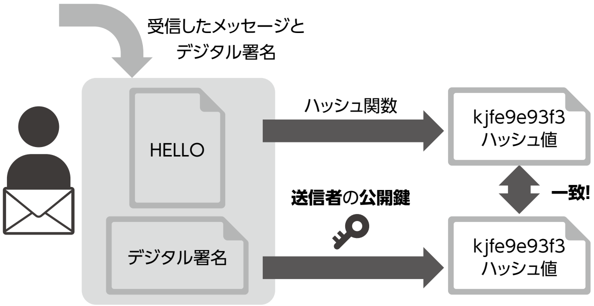
【受信者側の処理】

(1) 届いたデジタル署名を送信者の公開鍵を用いて元のハッシュ値に戻す。

(2) 届いたメッセージをハッシュ関数に入れてハッシュ値を求める。

(3) ハッシュ値を突き合わせて一致すれば，改ざんされていないこと・本人から届いたものであることが証明できる。

ここが POINT
改ざんの確認はハッシュ値のみでできるが，メッセージとハッシュ値の両方を改ざんされてしまうことを避けるため，公開鍵方式で暗号化している。

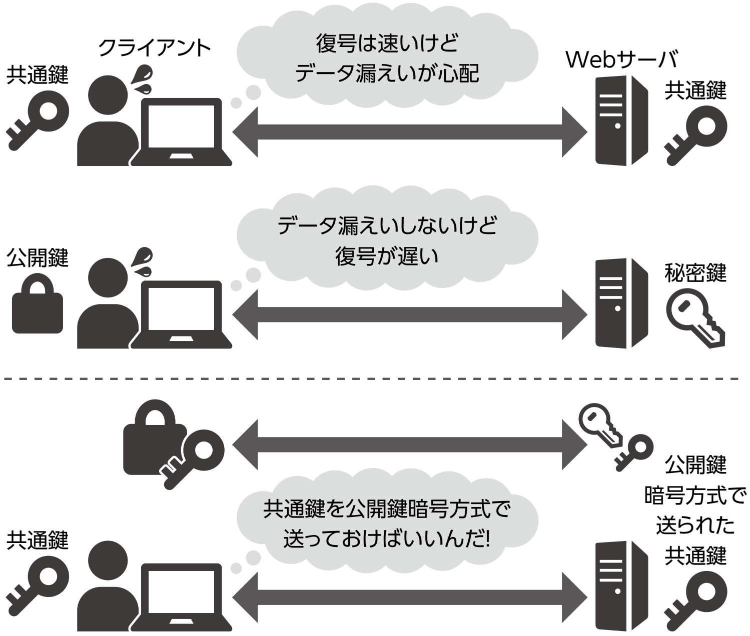


SSL/TLS

・SSL/TLS

Web ページにアクセスする時, ブラウザの URL 欄に「https://～」と一緒に鍵マークが表示されているのを見たことはないだろうか。

https は，〔⑫　　　　　　　　〕という技術を使って，通信経路上のデータを暗号化している。SSL/TLS は，暗号化技術を利用して，データの暗号化，改ざんの検知，認証の機能を提供するプロトコルである。SSL/TLS では，データの暗号化に共通鍵暗号方式が用いられ，その共通鍵の受け渡しに公開鍵暗号方式を用いている。



覚えておこう

TLS は SSL の後継のプロトコルである。SSL 自体は，暗号化したデータの解読方法が分かってしまっているため，現在はほとんど TLS に置き換わっている。SSL はかなり長い歴史を持っているので，TLS が使われていても，SSL と呼ばれることも多い。

知っておこう

ここでは処理を簡単に説明するために省略しているが，通常，公開鍵は認証局（CA）が発行するデジタル証明書に添付されて送られてくる。受信側は，デジタル証明書を検証することでサーバが本物である（信頼できる）ことを確認できる。

知っておこう

SSL/TLS にはさまざまなバージョンがあり，ここではその仕組みの一例を紹介している。

まとめ

- **共通鍵暗号方式**は，暗号化に使う鍵と復号に使う鍵が同じ暗号化方式である。
- **公開鍵暗号方式**は，公開鍵と秘密鍵を使って暗号化・復号する暗号化方式である。
- **デジタル署名**は，送信されてきたデータが間違いなく本人（送信者）のものであること，改ざんされていないことを証明するための技術である。
- **SSL/TLS** は，暗号化技術を利用して，データの暗号化，改ざんの検知，認証の機能を提供するプロトコルである。

＜MEMO＞

Chapter2　実践問題

問 1　次のア～エの説明は，「共通鍵暗号方式」と「公開鍵暗号方式」のどちらによく当てはまるか，それぞれ答えなさい。

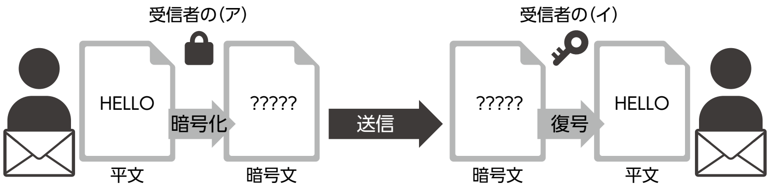
ア　暗号化と復号に用いる鍵が別である。

イ　もう一方の方式と比較して，暗号化と復号が高速に行える。

ウ　もう一方の方式と比較して，鍵の受け渡しが困難である。

エ　暗号化と復号に使ういずれの鍵も秘密の情報であるため，厳重に管理しなければならない。

問 2　以下の図は，公開鍵暗号方式の処理の流れを表したものである。受信者側で公開鍵と秘密鍵の鍵ペアを作成している。空欄（ア）（イ）には「公開鍵」「秘密鍵」いずれの用語が当てはまるか答えなさい。



問 3　次のア～エのハッシュ値の説明について，正しければ○，誤っていれば×で答えなさい。また，誤っているものは何が誤っているか説明しなさい。

ア　同じデータをハッシュ関数にいれた場合，求められるハッシュ値は必ず同じになる。

イ　ハッシュ値はメッセージダイジェストとも言い，元のデータが容易に推測できる。

ウ　元のデータを一文字変えると求められるハッシュ値も 1 文字変わる。

エ　デジタル署名は，送信する文書のハッシュ値を秘密鍵で暗号化（署名）したものである。

問 4　SSL/TLS に関する，次のア～エの説明について，正しければ○，誤っていれば×で答えなさい。また，誤っているものは何が誤っているか説明しなさい。

ア　TLS は SSL の後継にあたり，現在は，TLS を利用するのが主流である。

イ　データを暗号化するための鍵の交換に共通鍵暗号方式を利用し，データの暗号化に公開鍵暗号方式を利用する。

ウ　公開鍵が本物であることは，認証局（CA）が発行するデジタル証明書を用いて検証する。

エ　URL が「http:// ～」の場合はこの SSL/TLS 技術が使われ，暗号化通信が行われている。

第8講　PART5　確認問題

問 1　データのやり取りでは，第三者に盗聴されることを防ぐため，データの内容を暗号化して送信する。暗号化の方法には主に（　ア　）と（　イ　）の二つがある。（　ア　）は暗号化と復号のどちらにも同じ鍵を使用する方法で，鍵の管理を慎重に行う必要がある。（　イ　）は，外部に漏洩しても問題のない（　ウ　）と，受信者のみが持っている（　エ　）の組み合わせで暗号化と復号を行う。

(1)　空欄（ア）に入る語句として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　共通鍵暗号方式　　②　公開鍵暗号方式
③　デジタル署名　　④　ハッシュ化

(2)　空欄（イ）に入る語句として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　共通鍵暗号方式　　②　公開鍵暗号方式
③　デジタル署名　　④　ハッシュ化

(3)　空欄（ウ）に入る語句として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　公開鍵　　②　デジタル署名
③　ハッシュ値　　④　秘密鍵

(4)　空欄（エ）に入る語句として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　公開鍵　　②　デジタル署名
③　ハッシュ値　　④　秘密鍵

問２　元のデータを与えて，一定の長さの値に変換することを（　ア　）といい，その値をハッシュ値という。ハッシュ値から元のデータに戻すことはできず，元のデータから少しでも変化があると全く違う値に変わるため，a デジタル署名の技術に利用されている。

(1)　空欄（ア）に入る語句として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　暗号化　　②　デジタル署名
③　ハッシュ化　　④　復号

(2)　下線部 a に関する説明として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　デジタル署名では，データの改ざんを検知するためにハッシュ値を利用している
②　デジタル署名とは，データ送信者の名前を暗号化したものである
③　届いたデジタル署名は，秘密鍵を用いて復号する
④　デジタル署名とは，データ受信者の名前を暗号化したものである

問３　https を利用すると，http に比べて安全性の高い通信が可能である。https の安全性を高めるために使われているプロトコルの名称として最も適切なものを，次の①～④のうちから一つ選びなさい。

①　FTP　　②　IMAP
③　SSL/TLS　　④　TCP/IP

第 8 講　情報通信ネットワーク

PART1　ネットワーク

問 1　（ア）②　（イ）④　（ウ）①　（エ）③

問 2　（ア）サーバ　（イ）クライアント　（ウ）サーバ

問 3　省略

PART2　プロトコル

問 1　（ア）②　（イ）①　（ウ）④　（エ）③

問 2　IP アドレスはドットを境に 8 ビット単位なので，10 進法では 0 ～ 255 の範囲となる。よって，258 の部分はあり得ない数値である。

問 3　（ア）×　UDP は再送制御を行わない。

（イ）×　双方に互換性がないことから，まだ IPv6 への移行途中の段階。

（ウ）×　ルータのルーティングによって，それぞれのパケットごとに違う経路の場合もある。

PART3　WWW とメール

問 1　④→②→③→①

問 2　（ア）×　（イ）×　（ウ）○　（エ）×

問 3　（ア）SMTP　（イ）SMTP　（ウ）POP

問 4　「ドメイン名は, DNS サーバの住所」の部分が誤り。この会話でのドメイン名は，DNS サーバの住所ではなく Web サーバの住所が正しい。

PART4　情報セキュリティ

問 1　（ア）可用性　（イ）機密性　（ウ）完全性

問 2　ファイアウォールで食い止められない不正アクセスも多々あり，定期的なルールの見直しも必要である。

問 3　サイト A およびサイト B は閲覧できるが，それ以外のサイトの閲覧はフィルタリングルールにより拒否される。

問 4　（ア）×　（イ）○　（ウ）×　（エ）○

PART5　暗号化とデジタル署名

問１　（ア）公開鍵暗号方式　（イ）共通鍵暗号方式

（ウ）共通鍵暗号方式　（エ）共通鍵暗号方式

問２　（ア）公開鍵　（イ）秘密鍵

問３　（ア）○

（イ）×　ハッシュ値から，元のメッセージを推測することは困難である。

（ウ）×　元のメッセージが１文字でも異なれば，全く異なるハッシュ値となる。

（エ）○

問４　（ア）○

（イ）×　共通鍵を受け渡すための鍵交換には公開鍵暗号方式を使い，その後のやり取りするデータの暗号化には，公開鍵暗号方式より高速な共通鍵暗号方式を用いるのが正しい。

（ウ）○

（エ）×　URL が「http:// ～」の場合は，通信経路が暗号化されていない。

PART6　情報システムとデータベース

問１　ウ

問２　（ア）C to C　（イ）B to C　（ウ）B to B

問３　（ア）○　（イ）○　（ウ）×　（エ）○

PART7　データベース管理システム

問１　（ア）×　（イ）○　（ウ）○　（エ）×

問２　（ア）③　（イ）①　（ウ）②

問３　（ア）①，②，③　（イ）①，②　（ウ）①

第 8 講　PART5　確認問題　解答

問 1

(1) ①

解説：

共通鍵暗号方式では暗号化と復号に同じ鍵を使用する。

(2) ②

解説：

公開鍵暗号方式では暗号化と復号で別々の鍵を使用する。

(3) ①

解説：

暗号化のみに使用する公開鍵は，外部に公開しても問題ない。

(4) ④

解説：

復号に使用する秘密鍵は，外部に公開してはいけない。

問 2

(1) ③

解説：

元のデータからハッシュ値を生成することを，ハッシュ化という。

(2) ①

解説：

復号したハッシュ値が一致すれば，送信者が本人であることと，送信内容が改ざんされていないことが確認できる。

問 3　③

解説：

https は，SSL/TSL というプロトコルによって暗号化された通信を利用している。